

### Amendments to the Claims

1 Claim 1 (original): A security container that secures a document component by encapsulating,  
2 within the security container, the document component, conditional logic for controlling  
3 operations on the document component, and key distribution information usable for controlling  
4 access to the document component.

1 Claim 2 (original): The security container according to Claim 1, wherein the security container  
2 secures a portion of a higher-level document.

1 Claim 3 (original): The security container according to Claim 2, wherein the higher-level  
2 document has more than one portion secured by security containers.

1 Claim 4 (original): A method of securing document content using security containers,  
2 comprising the step of encapsulating, within a security container, a document component,  
3 conditional logic for controlling operations on the document component, and key distribution  
4 information usable for controlling access to the document component.

1 Claim 5 (original): The method according to Claim 4, wherein the key distribution information  
2 further comprises an identification of one or more users and/or processes that are authorized to  
3 access the document component.

1 Claim 6 (original): The method according to Claim 5, wherein the key distribution information

2 further comprises a symmetric key that encrypted both the document component and the  
3 conditional logic that are encapsulated within the security container, wherein the symmetric key  
4 is stored in an encrypted form for decryption by the authorized users and/or processes.

1 Claim 7 (original): The method according to Claim 6, wherein the encrypted form of the  
2 symmetric key comprises a separate version of the key for each distinct user, process, group of  
3 users, or group of processes, wherein the separate version has been encrypted with a public key  
4 associated with the corresponding distinct user, process, group of users, or group of processes.

1 Claim 8 (original): The method according to Claim 5, wherein the authorized users and/or the  
2 authorized processes are specified individually or as groups.

1 Claim 9 (original): The method according to Claim 4, wherein the conditional logic further  
2 controls access to the document component.

1 Claim 10 (original): The method according to Claim 9, wherein the key distribution information  
2 further controls access to the conditional logic.

1 Claim 11 (original): The method according to Claim 4, wherein the document component and  
2 the conditional logic are encrypted before encapsulation within the security container.

1 Claim 12 (original): The method according to Claim 4, wherein the security container is encoded

2 in structured document format.

1 Claim 13 (original): The method according to Claim 12, wherein the structured document format  
2 is Extensible Markup Language (“XML”) format.

1 Claim 14 (original): The method according to Claim 5, wherein the identification of the one or  
2 more users and/or processes comprises an identification of at least one group, the group having  
3 as members one or more of the users and/or processes.

1 Claim 15 (original): The method according to Claim 14, wherein the members are determined  
2 dynamically, upon receiving a request to access to the document component.

1 Claim 16 (original): The method according to Claim 15, wherein the dynamic determination  
2 further comprises accessing a repository where the members of the group are identified.

1 Claim 17 (original): The method according to Claim 4, further comprising the steps of:  
2 receiving, from a requester, a request to access the document component;  
3 programmatically determining, using the key distribution information, whether the  
4 requester is authorized to access the document component; and  
5 programmatically evaluating, using the conditional logic, whether the request can be  
6 granted, when the programmatically determining step has a positive result, and rejecting the  
7 request when the programmatically determining step has a negative result.

1 Claim 18 (original): The method according to Claim 17, wherein the conditional logic evaluates  
2 at least one of: an identity of the requester; a device used by the requester; a context of the  
3 requester; a zone of an application used by the requester; a user profile of the requester; and a  
4 target destination of the request.

1 Claim 19 (original): A computer program product for securing document content using security  
2 containers, the computer program product embodied on one or more computer-readable media  
3 and comprising:

4 computer-readable program code means for receiving, from a requester, a request to  
5 access document content, wherein the document content is encapsulated as a document  
6 component within a security container along with conditional logic for controlling operations on  
7 the document component and key distribution information usable for controlling access to the  
8 document component;

9 computer-readable program code means for programmatically determining, using the key  
10 distribution information, whether the requester is authorized to access the document component;  
11 and

12 computer-readable program code means for programmatically evaluating, using the  
13 conditional logic, whether the request can be granted, when operation of the computer-readable  
14 program code means for programmatically determining yields a positive result, and for rejecting  
15 the request when operation of the computer-readable program code means for programmatically  
16 determining yields a negative result.

1 Claim 20 (original): A system for securing document content using security containers,

2 comprising:

3 a security container that encapsulates a document component, conditional logic for  
4 controlling operations on the document component, and key distribution information usable for  
5 controlling access to the document component;

6 means for receiving, from a requester, a request to access the document component;

7 means for programmatically determining, using the key distribution information, whether  
8 the requester is authorized to access the document component; and

9 means for programmatically evaluating, using the conditional logic, whether the request  
10 can be granted, when operation of the means for programmatically determining yields a positive  
11 result, and for rejecting the request when operation of the means for programmatically  
12 determining yields a negative result.

1 Claim 21 (original): The system according to Claim 20, wherein the security container is  
2 embedded within a document.

1 Claim 22 (original): The system according to Claim 20, wherein the security container  
2 encapsulates the document component on a system clipboard.

1 Claim 23 (original): The system according to Claim 20, wherein the security container is placed  
2 on a user interface.

1 Claim 24 (original): The system according to Claim 20, wherein the security container  
2 encapsulates the document component for exchange using interprocess communications.

1 Claim 25 (original): The system according to Claim 20, wherein the security container  
2 encapsulates the document component for exchange using a messaging system.

1 Claim 26 (original): The system according to Claim 20, further comprising means for copying  
2 the document component to a target destination, wherein the means for copying copies the entire  
3 security container in order to copy the document component.

1 Claim 27 (original): A method of securing document content using security containers,  
2 comprising steps of:

3 receiving, from a requester, a request to access document content, wherein the document  
4 content is encapsulated as a document component within a security container along with  
5 conditional logic for controlling operations on the document component and key distribution  
6 information usable for controlling access to the document component;

7 programmatically determining, using the key distribution information, whether the  
8 requester is authorized to access the document component;

9 programmatically evaluating, using the conditional logic, whether the request can be  
10 granted, when the programmatically determining step has a positive result, and for rejecting the  
11 request when the programmatically determining step has a negative result; and

12 charging a fee for carrying out one of more of the receiving, programmatically  
13 determining, and programmatically evaluating steps.

1 Claim 28 (original): A method of securing document content using security containers,  
2 comprising steps of:

3 receiving, from a requester, a request to access document content, wherein the document  
4 content is encapsulated as a document component within a security container along with  
5 conditional logic for controlling operations on the document component and key distribution  
6 information usable for controlling access to the document component;

7 programmatically determining, using the key distribution information, whether the  
8 requester is authorized to access the document component;

9 programmatically evaluating, using the conditional logic, whether the request can be  
10 granted, when the programmatically determining step has a positive result, and for rejecting the  
11 request when the programmatically determining step has a negative result; and

12 charging a fee to the requester when the programmatically evaluating step determines that  
13 the request can be granted.

1 Claim 29 (new): The method according to Claim 5, further comprising the steps of:

2 sending the security container to one or more recipients; and

3 upon receipt at each of the recipients, using the conditional logic to determine whether  
4 that recipient can access the document component encapsulated within the security container.

1 Claim 30 (new): The method according to Claim 5, further comprising the steps of:  
2 receiving, at a recipient, the security container; and  
3 using the conditional logic to determine whether the recipient can access the document  
4 component encapsulated within the security container.

1 Claim 31 (new): The method according to Claim 5, further comprising the steps of:  
2 receiving, at a plurality of recipients, the security container; and  
3 using the conditional logic, at one or more of the recipients, to determine whether that  
4 recipient can access the document component encapsulated within the security container.

1 Claim 32 (new): The method according to Claim 4, wherein the security container encapsulates  
2 the document component for transfer to a plurality of members of a group, and wherein  
3 each member of the group to which the transfer is made uses the conditional logic for  
4 determining whether that member is authorized to access the document component.